Volume 2, No.6, June, 2026

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

RESEARCH PAPER

Available online at http://www.jgrma.com

ROBUST DEEP LEARNING MODELS FOR SECURE NETWORK TRAFFIC ANALYSIS FOR IMPROVE CYBERSECURITY

Dr. Neetu Sikarwar
Department of Electronice Engineering
Institute of Engineeeirng , Jiwaji UniversityGwalior,India
Neetusik1@gmail.com

Abstract: The fast growth of internet-connected devices has made the cyber landscape more complicated and presents new challenges for security experts seeking intelligent and real-time solutions to combat these threats. A novel architecture for deep learning (DL) is proposed by this framework, which employs ML methods and analysis of network data to thwart cyber-attacks. This study presents a CNN and LSTM model-based DL-based network intrusion detection system (NIDS) that effectively uses the CICDDoS2019 dataset to address this issue. Before training a model efficiently, data must be preprocessed by removing unnecessary or redundant characteristics, normalizing it, encoding labels, and dividing it into a training and testing set. When it comes to accurate intrusion detection, CNN models are employed for automated spatial feature extraction, whereas LSTM models are used for modeling temporal and sequential traffic patterns. Accuracy (ACC) levels of 99.96% for a CNN model and 99.98% for an LSTM model were achieved in the experimental findings, which also demonstrated good Precision (PRE), Recall (REC), and F1 score (F1) values. Training and validation performance curves, as well as confusion matrix analysis, demonstrated that the proposed models are reliable and robust, with few classification errors and minimal overfitting. Additionally, the suggested framework is contrasted with alternative DL and ML techniques, which further prove its excellence in analyzing network data and detecting cyberattacks. The proposed system would enable effective and reliable cybersecurity monitoring in contemporary network environment.

Keywords: Network Intrusion Detection, Deep Learning, Cybersecurity, DDoS Attack Detection, Intrusion Detection System (IDS), Machine Learning.

1 INTRODUCTION

A common and costly kind of cyberattack, Distributed Denial of Service (DDOS) attempts to overwhelm a network or service with an overwhelming amount of data from several sources in an effort to knock it offline. A DDOS attack can be launched in several methods. One is to flood the network with requests or packets. Another is to exploit security vulnerabilities in the protocols or devices that control the network [1]. DDOS attacks are malicious cyberattacks that target specific websites, networks, or even people, and they can interrupt their operations, harm their reputation, or even steal their trust. One exciting concept that might make networks more secure and resistant to DDOS attacks is software-defined networking, or SDN. SDN allows for the centralization of control and administration of network resources.

A strong defines against harmful software attacks like denial of service (DoS) was proposed in 1980 with the Intrusion Detection System (IDS). When an intrusion attempts to mimic a DoS attack, intrusion detection systems (IDS) can detect it and block or halt the illegal traffic [2]. Typically, when a classification difficulty arises, intrusion detection is the answer [3]. The poor detection ACC of several current IDS is one of its drawbacks. Another problem is that they can't identify new attacks because they only use known ones [4]. There are two primary ways in which IDS may be put into place: on hosts or in networks. Network IDS monitors network traffic for signs of attacks. Alternatively, host-based intrusion detection systems just keep tabs on a single application or server [5]. Additionally, IDS provides two detection methods. One is signature-based, which compares real-time data to a repository that contains attack signatures.

IDS has benefited from the potential of AI to enable machines and computers to learn from datasets with little to no human involvement [6][7]. When designing and developing an efficient intrusion detection system, both ML and DL, which are branches of AI, are applied[8]. In a ML system, features are retrieved by hand and used for network traffic categorization and detection [9][10]. Different from ML, DL may improve the model's detection accuracy by training a neural network to sift through datasets in search of characteristic information before applying classification and detection.

Internet applications, cloud computing and connected devices are growing in number, leading to an escalation of cyber threats and DDoS attacks in today's networks [11][12][13]. Traditional intrusion detection methods can be ineffective at detecting sophisticated attack patterns and dealing with high volumes of network traffic efficiently. Hence, there is a need for intelligent DL -based techniques that can automatically learn network traffic behaviour and offer accurate and reliable intrusion detection for cybersecurity applications [14]. The key contributions offered by the study are discussed below:

- Proposed a DL-based network IDS framework based on CNN and LSTM model for network traffic analysis.

- Conducted data cleaning, normalization, feature selection, and label encoding on the CICDDoS2019 dataset as part of the comprehensive data pre-processing.
- Extracted the key spatial traffic features using CNN and learned the sequential and temporal traffic patterns using LSTM.
- Evaluated the detailed performance with the help of confusion matrix, ACC and loss analysis, PRE, REC, and F1.
- Validated the framework's efficacy and robustness by comparing the suggested models to existing ML and DL models.

This effort is justified by the increasing need for intelligent and dependable IDS to handle large-scale and complicated network traffic in the present cyber security situation. Traditional ML methods have a hard time detecting attack patterns with both spatial and temporal dimensions, leading to low detection efficiencies and high false classification rates. The suggested work is innovative because it employs CNNs with LSTM DL models to rapidly analyze CICDDoS2019 dataset network traffic. CNNs automatically detect important traffic features, and LSTMs learn sequential network traffic patterns. The suggested architecture uses effective pre-processing and evaluation approaches to boost detection robustness, overall cybersecurity monitoring capabilities, and detection accuracy to a greater extent.

The structure of the paper is as follows: In Section II, offer findings from the literature research and in-depth examination of current IDS methods. Section III lays forth the strategy that has been suggested. The experimental results and comparison with current models are discussed in Section IV. In Section V, the report comes to a close and suggests avenues for further study on sophisticated network IDS.

2 LITERATURE REVIEW

This article reviews a lot of research on how to use DL to find DDoS attacks during IDS. An experiment using datasets including DDoS attacks was summarized in this portion, along with several DL models.

S. U and Venkateshappa (2026) present the Multi-Scale Temporal Spike-Based Intrusion Detection System (MSTS-IDS), leveraging SNNs for energy-efficient multi- temporal pattern recognition. Experimental validation demonstrates 96.3 % detection ACC with 75% energy reduction compared to traditional approaches. The framework achieves 93.7% APT campaign detection ACC while maintaining sub-millisecond response times for fast attacks [15].

N. T. Gurram (2025) presents a novel IDS framework that is based on AI, particularly using DL-based architectures and network traffic characterization, to improve system performance and resilience. A number of different architectures were tried in order to process and evaluate using the CICIDS2017 dataset, including CNN, RNN, LSTM autoencoder. The LSTM model outperformed all others in terms of capturing the historical traffic temporal aspect, with an overall performance of 97.4% ACC, 96.2% REC, and 95.8%, according to the experimental data. CNN followed closely behind with 96.5 % ACC and 94.9 % REC and it is arguably the computationally efficient in real-time IDS detection [16].

RituRani (2025) proposed method consists in four phases: data collecting, data pre-processing, feature selection and extraction, and classifier application. The dataset is cleaned and normalized at the pre-processing step; next, in order to boost classification ACC, relevant features are selected. The training and evaluation of NB and SVM models for classification is followed by an evaluation of their efficacy using several performance measures, including ACC, PRE, REC, and F1. The results reveal that the SVM classifier has low misclassification and great ACC (97.29%), therefore proving its prospective use in advanced IDS [17].

N. Roy et al. (2025) using a dataset that includes both common and unusual network traffic patterns. The suggested model employs stacked ensemble learning with several base classifiers to improve detection. As a starting point, goes with RF, XGBoost, and SGD. These approaches are chosen as they can discriminate between regular and harmful network activity better. After integrating these basic learners, a meta-classifier refines the final predictions by learning from their collective outputs. With 94.4% ACC, the stacking ensemble technique detects network abnormalities better than individual models [18].

S. Kumar et al. (2024) provide a novel approach to malware identification and classification that use image visualization and employs ML and transfer learning classifiers. The first step is to convert the PCAPs from the network to grayscale. The next step is to add a multi-dimensional fully-connected layer to pre-trained CNN models like Xception, EfficientNetB0, VGG19, and EfficientNetB0 in order to train them to extract textural characteristics via transfer learning. The hyperparameter optimization of all classifiers is performed using grid search and randomized search algorithms. This study performs intensive experiments using 913 public image datasets, and the proposed method obtained 94.71% ACC, which is an excellent performance even using a smaller dataset [19].

D B. Zhang and X. Zhang (2024) using big data analysis, an Attention-based Hybrid DL model is proposed for IDS in network. Experimental results presented that the proposed Attention-based CNN-LSTM (Att-CNN-LSTM) achieved better detection ACC with 99.76%, PRE 97.62%, and F1 96.49% when compared with the traditional DL based IDS such as FSBDL and DCNN-BiLSTM [20].

3 RESEARCH METHODOLOGY

The methodology proposed for network intrusion detection in CICDDoS2019 dataset involves data collection, data pre-processing, modelling and performance evaluation. To enhance the data quality, the dataset is cleaned by removing unnecessary features related to the socket, null values and infinite values and subsequently normalized and label encoded. Training, validation, and testing sets of data were then created. Learned spatial and sequential traffic patterns are fed into DL models like CNN and LSTM, which are then used for attack detection. Lastly, the models' performance is evaluated by analyzing their training-validation performance for network

intrusion detection as well as by looking at their REC, ACC, PRE, F1, confusion matrix, and overall performance. In Fig 1, can see how the suggested approach would work

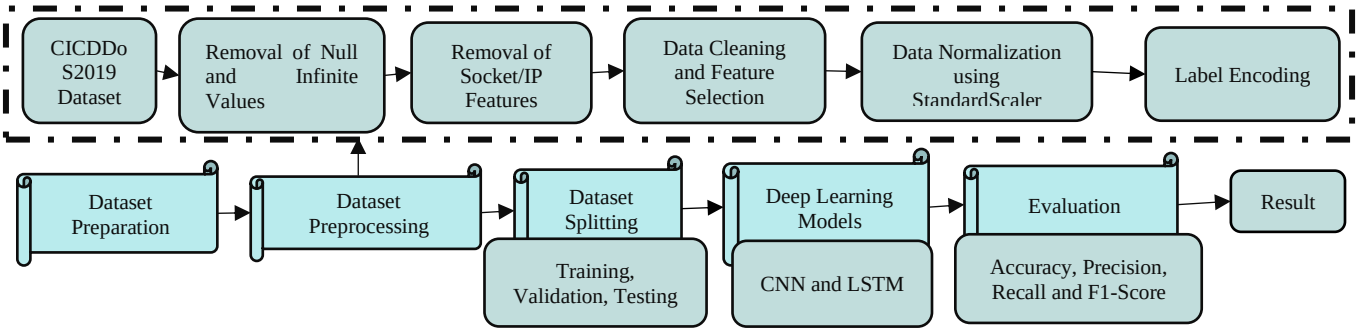

Figure.1. Sequence of Steps for Proposed Approach

The subsequent section details the process depicted in the proposed flowchart for intrusion detection.

3.1 Data Collection and Visualization

The CIC has assembled a large dataset called the CIC-DDoS2019 to aid in studies aimed at identifying and preventing DDoS assaults. The data collection contains several distinct types of DDoS attacks. Attacks employing botnets, HTTP, UDP, and TCP floods are all part of this category. This dataset is perfect for training and testing DDoS detection systems that rely on ML since it contains both legitimate and malicious traffic. Below is a graphic representation of the EDA of the datasets:

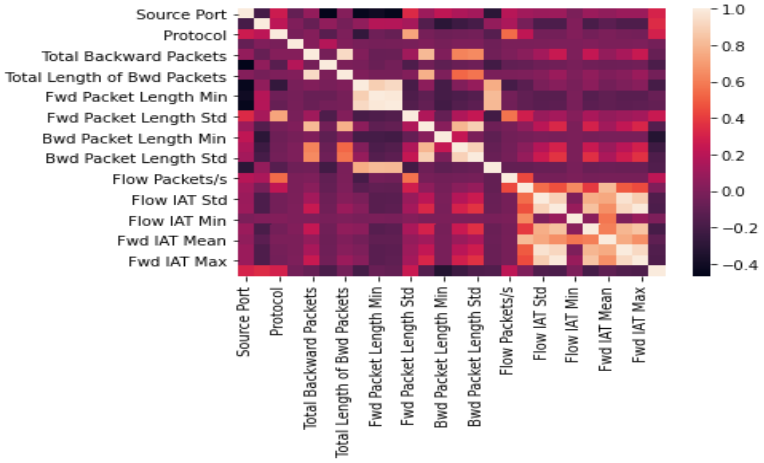

Figure.2. Correlation Heatmap of CICDDoS2019 Dataset Features

The correlation heatmap between the features derived from the network traffic for the IDS framework is shown in Fig. 2. The color intensities show the significance of the correlation of features, with brighter areas showing stronger positive relationships and darker areas showing weaker relationships. Heatmap is used to find the features which are highly correlated and to avoid redundancy in the feature selection and pre-processing. Fig. 3 displays the label distribution in the CICDDoS2019 dataset. The graph shows the sample sizes for each type of traffic and the variations in these classes between attack and non-attack traffic cases. This visualization is useful for analyzing data balance and also for effective pre-processing and training of the models for network intrusion detection.

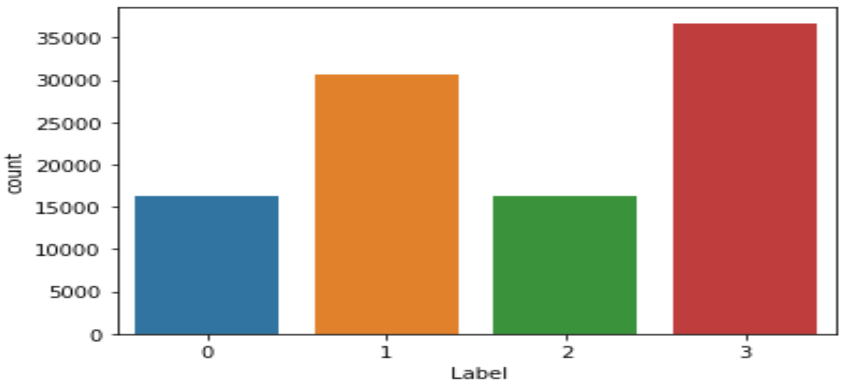

Figure.3. Count plot for label Distribution

3.2 Data Pre-Processing

There are a number of things that need to be done to prepare the data for the module training, but the end goal is to have it used directly by the training model. To achieve this, can obtain the CICDDoS2019 dataset in a flow-based format using CICFlowMeter, and extract over 80 attributes from it.

3.2.1 Removing remaining null values

The dataset has sufficient records to enable the elimination of non-numerical type null values, which cannot be replaced.

3.2.2 Removing socket features

This study does not include socket characteristics such as source and destination IP, port, date, and flow ID. Instead, the model needs to be trained with packet characteristics, which are different for each network. Another point is that the same IP address might belong to both the invader and legitimate users. Because the DL model may become biased when trained using socket information, overfitting becomes an issue. Following the elimination of superfluous characteristics, they generated 77 features to use as input to the model.

3.2.3 Cleaning the data

The original data has a lot of null and infinite numbers that need to be gotten rid of.

3.2.4 Normalize the input data

The characteristics of the chosen dataset are normalized by standard scalar normalization in order to detect attacks. The CICDDoS2019 dataset includes a variety of characteristics that vary in size, distribution, and dimensionality. Take the 'Fwd Packets/s' feature as an example; it has values that are modest for some records and extremely huge for others. The performance of DL models trained using these raw features is often low. It is derived in Equation (1):

$$x_n = \frac{x-\mu}{\sigma} \qquad (1)$$

The normalized value, denoted as xn, is calculated by taking the original value, an average of the data, and the standard deviation, denoted as μ, and adding them together.

3.2.5 Encoding the labeled data

ML and DL models work with numbers, which means that category values need to be turned into numbers. For the purpose of improving the model's performance, numerical values are assigned to categorical categories and character sets. Two techniques that can be used to transform categorical data into numerical data are label encoding and one-hot encoding. Label encoding is a method that uses unique numerical labels to transform categorical input into numerical data. An sklearn module named LabelEncoder is available for usage in converting categorical data to numerical form.

3.3 Dataset Splitting

Training data, validation data, and testing data often make up the training model after the dataset (80:10:10).

3.4 DDoS Detection Models

This part talks about the suggested deep learning models, which are CNNs and LSTM networks:

3.4.1 Convolutional Neural Networks (CNNs)

Automatic training on the CICDDoS2019 dataset prepares the proposed CNN model to detect network intrusions with minimal network overhead. The model starts with max-pooling and dense classification layers, then it moves on to many convolutional layers that utilize ReLU activation functions [21]. Achieving peak performance requires fine-tuning the following hyperparameters: 20 training epochs, a categorical cross-entropy loss function, an Adam optimizer, and 32 batches make up this model's parameters. The introduction of dropout layers further helps reduce overfitting and enhances generalizability. The CNN model has obtained excellent ACC and IDS performance with few errors in classification.

3.4.2 Long Short-Term Memory (LSTM)

ANNs are widely used in the field of DL, and one variant or improved form of this architecture is LSTM [22]. Training the suggested LSTM model for intrusion detection on the CICDDoS2019 dataset requires it to understand the sequential patterns and temporal correlations inherent in the network traffic data. Using a stack of LSTM layers and dense fully-connected layers, the design achieves categorization functionality. The activation functions that are used are ReLU and Softmax. A 32-batch size and a 0.001 Adam optimizer learning rate are all that's needed after 20 training rounds with the categorical cross-entropy loss function. Enhance the model's capacity to generalize and reduce the risk of overfitting by using dropout regularization. Experiment findings demonstrated that LSTM model outperformed other models in classifying harmful network activity, with high values for ACC, PRE, REC, and F1.

3.5 Evaluation Metrics

There are four metrics used to measure the ACC of classification algorithms: ACC, PRE, REC, and F1:

3.5.1 Accuracy

The accuracy of DDoS attack detection in the dataset, or ACC, is determined using Equation (2).

$$Accuracy = \frac{TP+TN}{P+N} \quad (2)$$

3.5.2 Precision

The PRE is calculated using Equation (3) and it represents the percentage of correctly diagnosed DDoS attacks relative to all occurrences labeled as DDoS.

$$Precision = \frac{TP}{TP+FP} \quad (3)$$

3.5.3 Recall

The ability to accurately categorize DDoS traffic is measured by REC, which is computed using Equation (4).

$$Recall = \frac{TP}{TP+FN} \quad (4)$$

3.5.4 F1-score

F1 is a performance measure that equalizes PRE (A) and REC (B) using a harmonic mean, as shown in Equation (5)

$$F1 = \frac{2\times precision\times recall}{precision+recall} \quad (5)$$

The four pillars upon which these assessment tools rest are: The sum of all identified instances of typical traffic; Quantity of incorrectly classified DDoS packets; Number of FP, the overall tally of mislabelled DDoS traffic incidents; and Number of FN, the overall tally of mislabelled regular traffic instances.

4 RESULTS AND DISCUSSION

The model was created using specifications from a Dell Inspiron 15 3511 with 8.00 GB of RAM and a 2.80 GHz Intel(R) Core (TM) i7-1165G7 CPU. Use the TensorFlow, Pandas, and Keras packages to get the DL model running. Table 1 displays the results obtained from the CICDDoS2019 dataset using the suggested CNN and LSTM network intrusion detection models. Classification ACC scores exceeding 99.9% were produced by both models. When compared to the LSTM model, the CNN model performed better in terms of REC, F1, and total ACC. The outcomes demonstrate the high efficacy and dependability of the DL models suggested in the article for identifying cyber-attacks and network intrusions.

TABLE.1 PERFORMANCE RESULTS OF THE PROPOSED MODELS FOR NETWORK INTRUSION DETECTION ON CICDDOS2019 DATASET

Models	Accuracy	Precision	Recall	F1-Score
CNN	0.9996	0.9997	0.9999	0.9898
LSTM	0.9998	0.9996	0.9965	0.9998

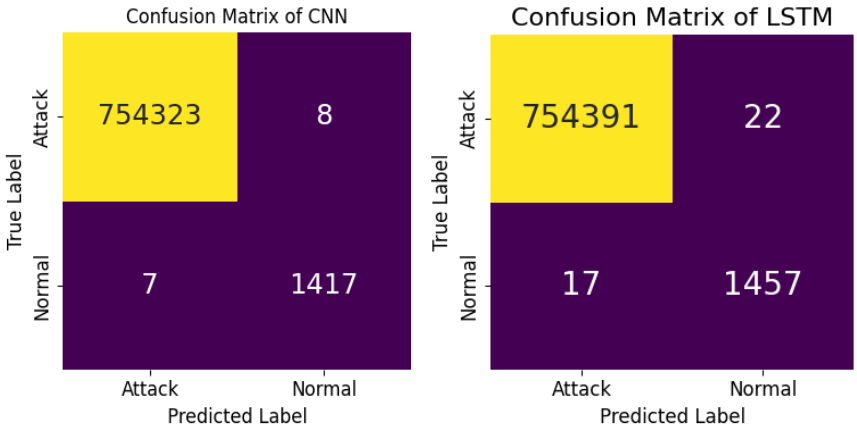

Figure.4. Confusion Matrix of the CNN and LSTM Model

The CNN and LSTM models utilized for attack categorization have their confusion matrices displayed in Fig. 4. The confusion matrix pertaining to the attack classification models of the CNN and LSTM. Classifying 754,323 attack instances and 1,417 normal cases with just 8 false positives and 7 FN revealed the CNN model's extraordinarily high ACC. Likewise, the LSTM model also showed good classification results with 754,391 correctly classified attack samples and 1,457 correctly classified normal samples; 17 false negatives and 22 false positives are recorded. The results show that both DL models are very efficient in the classification of attack and normal network traffic, with the LSTM model having a slightly better overall detection ability, and a higher percentage of correct normal instances.

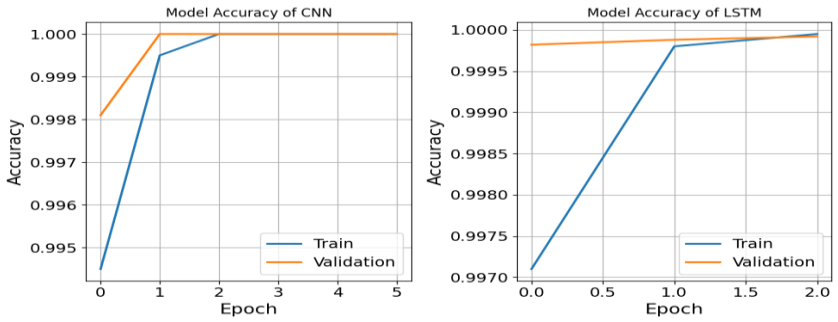

Figure.5. Training and Validation curve of CNN and LSTM models

Fig. 5 displays the ACC curves as they were trained and validated for the LSTM and CNN models. With consistent learning and high generalization, the CNN model rapidly converged to approximately 99%, with training and validation ACC coming extremely close to each other after just a few epochs. Likewise, the LSTM model showed a steady increase in ACC when training, with the validation ACC also staying very high throughout the epochs. It can be observed that both models show a close agreement between training and validation curves, indicating a good model performance without overfitting and validating the robustness of the proposed DL architectures for accurate attack detection and classification.

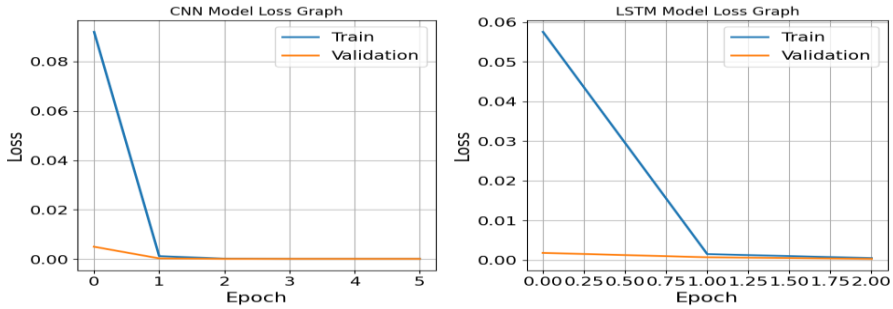

Figure.6. Training and Validation loss graph of CNN and LSTM

During training and validation, Fig. 6 shows the loss curves of the CNN and LSTM. Consistently low validation loss and a sharp decline in training loss in the CNN model from the first epoch onwards indicate effective training, model convergence, and steady learning performance. Likewise, the training loss for the LSTM model gradually decreased with training epochs while the validation loss is small during the training process. The loss curves of both models converged well and showed a downward trend in loss as time went on, indicating that they are able to reduce the errors in their predictions without overfitting. The outcomes demonstrate the potential of CNN and LSTM models to perform reliable and accurate in network attack detection tasks.

4.1 Comparative Analysis

Table 2 compares the suggested CNN and LSTM models to the current models in terms of their ability to analyze network traffic. The traditional models (DT, SVM, XGBoost, ANN) obtained good classification performance and the hybrid models (Voting Classifier) achieved better performance. The proposed CNN and LSTM models, however, achieved higher ACC rate of 99.96% and 99.98% respectively, than all the existing approach. The results show high PRE, REC, and F1, indicating high ACC, reliability, and efficiency in detecting attacks in the proposed DL models.

TABLE. 2 PERFORMANCE OF COMPARISON BETWEEN EXISTING AND PROPOSED MODELS FOR NETWORK TRAFFIC ANALYSIS

Models	Accuracy	Precision	Recall	F1-score
DT [23]	0.974	0.974	0.974	0.974
SVM [24]	0.8721	0.8718	0.8780	0.8718
Autoencoder-CNN-LSTM[25]	0.830	0.805	0.830	0.811
Voting Classifier[25]	0.998	0.998	0.998	0.998
XGBoost[26]	0.9845	0.9838	0.984	0.9842
ANN[27]	0.78	0.96	0.6205	0.7557
CNN	0.9996	0.9997	0.9999	0.9898
LSTM	0.9998	0.9996	0.9965	0.9998

The CNN and LSTM models proposed in this work are effective models for network traffic analysis and cyberattack detection because they can learn complex traffic patterns automatically from the set of network traffic. Network traffic can be modeled in a sequential and temporal relationship using the LSTM model, and geographical information can be extracted via the CNN model. The ACC, PRE, REC and f1 values obtained in both models are very high, which shows that both models have good and strong performance. The suggested method also reduces the possibility of false classification, increases detection capability and increases the effectiveness of cybersecurity monitoring.

4.2 Deep Analysis of Literature Study

The literature study shows that DL and ML approaches play an important role in intrusion detection and DDoS attack classification. Several models such as CNN, LSTM, SNN, ensemble learning, and hybrid architectures achieved strong detection performance on different cybersecurity datasets. However, many existing methods still face challenges related to computational complexity, real-time adaptability, and effective learning of both spatial and temporal traffic patterns. Therefore, the proposed CNN and LSTM-based framework is developed to provide accurate, reliable, and efficient network intrusion detection with improved attack classification capability.

5 CONCLUSION AND FUTURE STUDY

A DDoS assault is a powerful method used to target network devices and services; it has lately been considered a major attack. Consequently, this study will investigate DDoS assaults, evaluate them, and build a ML model to identify them. Using the CICDDoS2019 dataset and a CNN model and a LSTM model, this study develops a robust framework for network IDS using DL. The suggested models have exceptional proficiency in understanding intricate patterns of network traffic, exhibiting exceptional ACC, PRE, REC, and F1 in detecting attacks. Both models demonstrated dependable and strong performance with incredibly low misclassification rates, according to the experimental data. When compared to other suggested ML and DL models, the results revealed that the CNN and LSTM models performed better in analyzing network data and detecting intrusions. Indeed, as cyber threats are evolving, there is a need for advanced and adaptive intrusion detection techniques for real-world security applications. The proposed framework can be further optimized in the future by combining DL and attention mechanisms, which can further enhance detection ACC and reduce computational complexity. For practical cybersecurity monitoring, real-time deployment to cloud, IoT and edge computing is also a good idea. In addition, the combination of explainable AI, federated learning, and advanced feature optimization techniques could enhance the system's scalability, its explain ability, and its ability to withstand new and zero-day cyber threats.

REFERENCES

[1] I. A. Abdulmajeed and I. M. Husien, “MLIDS22- IDS Design by Applying Hybrid CNN-LSTM model on Mixed-Datasets,” *Informatica*, vol. 46, no. 8, Nov. 2022, doi: 10.31449/inf.v46i8.4348.

[2] M. Kumar and M. K. Shah, “AI-Driven DDoS Detection for Network Security: A Performance Analysis of Machine-Deep Learning Methods on Network Traffic Data,” in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395710.

[3] M. Kari, “Deep Learning-Based Fault Prediction Models for Enhanced Network Security Monitoring,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, p. 492, Jun. 2023, doi: 10.48175/IJARSCT-11600I.

[4] V. K. Bollu, “Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications,” *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr.2026.29.1.0007.

[5] D. Jain and S. Jain, “Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security,” in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395685.

[6] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, “CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System,” *IEEE Access*, vol. 10, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[7] T. A. Khan *et al.*, “Multi-Source Cyber Intrusion Detection Using Ensemble Machine Learning,” *J. Comput. Sci.*, vol. 21, no. 1, pp. 111–123, Dec. 2024, doi: 10.3844/jcssp.2025.111.123.

[8] S. Singh, “Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation,” in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[9] B. Madupati, M. M. Mohammed, L. Upadhyay, D. P. Guda, K. Kaushik, and M. Soni, “Integrating Artificial Intelligence with Cybersecurity for Resilient Wireless Communication Against Advanced Threats,” in *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, IEEE, Aug. 2025, pp. 1–5. doi: 10.1109/AIMV66517.2025.11203666.

[10] H. P. Cyril and S. Kumara, “Identification of Anomalies via Deep Learning - Based Models for High - Dimensional Telecom Traffic Data,” *J. Adv. Artif. Intell.*, vol. 4, no. 1, pp. 24–37, 2026, doi: 10.18178/JAAI.2026.4.1.24-37.

[11] V. K. Sharma, “Cloud Computing IoT: 5G Focused IoT with Cloud Solutions,” *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 6, no. 3, 2025, doi: 10.63282/3050-9416.IJAIBDCMS-V6I3P103.

[12] D. Bhattacharjee, “Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring,” in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[13] S. K. Chintagunta and S. Amrale, “Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 756–768, 2022.

[14] R. rao Thallada and N. Alapati, “Privacy and Cybersecurity Convergence: GRC Controls for Data Protection,” *ournal Bus. Manag. Stud.*, vol. 8, no. 5, pp. 42–48, March, 2026, doi: 10.32996/jbms.

[15] S. U and Venkateshappa, "Multi-Scale Temporal Spike-Based Intrusion Detection: A Novel Framework for Cybersecurity Applications," in *2026 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/IITCEE67948.2026.11394649.

[16] N. T. Gurram, "AI-Based Intrusion Detection Systems Using Deep Learning and Network Traffic Analysis," in *2025 OITS International Conference on Information Technology (OCIT)*, IEEE, Dec. 2025, pp. 492–497. doi: 10.1109/OCIT66168.2025.11400454.

[17] RituRani, "Next-Generation Intrusion Detection Systems with Machine Learning and Deep Learning-Based Firewalls," in *2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, IEEE, Jan. 2025, pp. 1–4. doi: 10.1109/IITCEE64140.2025.10915227.

[18] N. Roy, R. G. Tiwari, and S. Roy, "Stacking-Based Machine Learning Approach for Anomaly Detection in Embedded System Network Traffic," in *2025 Fourth International Conference on Smart Technologies, Communication and Robotics (STCR)*, 2025, pp. 1–6. doi: 10.1109/STCR62650.2025.11019443.

[19] S. Kumar, Y. Sapru, and K. Purushottama Rao, "Feature Fusion for Malware Traffic Detection Using Image Visualization and Transfer Learning," in *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Apr. 2024, pp. 993–998. doi: 10.1109/ICCSP60870.2024.10544220.

[20] B. Zhang and X. Zhang, "Big Data Analysis for Intrusion Detection System in Network with Attention based Hybrid Deep Learning Model," in *2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC)*, IEEE, Sep. 2024, pp. 1–5. doi: 10.1109/ICDSCNC62492.2024.10939312.

[21] U. Anthony. O, "CNN-based Network Intrusion Detection and Classification Model for Cyber-Attacks," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 7, pp. 1839–1847, Aug. 2024, doi: 10.38124/ijisrt/IJISRT24JUL1158.

[22] S. Shende, "Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security," *Int. J. Eng. Res.*, vol. V9, no. 06, Jul. 2020, doi: 10.17577/IJERTV9IS061016.

[23] Y. Alotaibi and M. Ilyas, "Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security," *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125568.

[24] B. S. Omarov, O. A. Auelbekov, B. O. Kulambayev, and B. S. Omarov, "Iot Network Intrusion Detection Using Machine Learning on UNSW-NB15 Dataset," *Her. Kazakh-British Tech. Univ.*, vol. 21, no. 3, pp. 48–57, Oct. 2024, doi: 10.55452/1998-6688-2024-21-3-48-57.

[25] A. Kalidindi, B. R. Koti, C. Srilakshmi, K. M. Buddaraju, A. R. Kandi, and G. S. S. Makutam, "Advanced Machine Learning Techniques for Enhancing Network Intrusion Detection and Classification Using DarkNet CIC2020," *Int. J. Online Biomed. Eng.*, vol. 20, no. 15, pp. 141–154, Dec. 2024, doi: 10.3991/ijoe.v20i15.50873.

[26] S. K. Mandal, A. K. Marandi, J. Gandhi, S. Loonkar, P. Dey, and S. Kaur, "Novel ML-driven intrusion detection system for optimizing network security," *Expert Syst. Appl.*, vol. 292, p. 128621, Nov. 2025, doi: 10.1016/j.eswa.2025.128621.

[27] M. Gopalsamy, "Enhanced Cybersecurity for Network Intrusion Detection System Based Artificial Intelligence (AI) Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 12, no. 01, pp. 671–681, Dec. 2021, doi: 10.48175/IJARSCT-2269M.

